## **Amendments to the Claims**

The following listing of claims replaces all previous versions of the claims.

1. (**Cancelled**)

2. (**Previously presented**) The system of claim 21 further comprising of a filtering module installed at the at least one server for blocking unauthorized processes in accordance with determined authorization level.

3. (**Currently Amended**) The system of claim 21 further comprising at least one agent installed on the at least one server, said agent enables correlating between processes and sessions on different servers, wherein the identity code is transferred between internal processes running on different servers.

4. (**Previously presented**) The system of claim 21, wherein each the additional process comprises a process information vector, and the module associates the identification code of the original session to the additional process by adding the session identification code to the  information vector of the additional process.

5. (**Previously presented**) The system of claim 4 wherein the session identification code replaces redundant information in the process information vector.

6. (**Previously presented**) The system of claim 21 wherein the processes operated by each original session are associated to the original session's identification code by a unique process identifier.

7. (**Previously presented**) The system of claim 21 wherein the original session properties are sign in parameters.

8. (**Previously presented**) The system of claim 21 wherein the original session properties are initial session type parameters.

9. (**Previously presented**) The system of claim 21 wherein the original session properties are hyperlink session address type parameters.

10. (**Previously presented**) The system of claim 21 wherein the original session is identified according to a unique Transmission Control Protocol (TCP) port ID.

11. (**Cancelled**)

12. (**Previously presented**) The method of claim 22 further comprising the step of filtering processes in accordance with the determined authorization level associated with the session identification code of each process.

13. (**Currently Amended**) The method of claim 22 further comprising the step of correlating between process and sessions on different servers within the server network environment, wherein the identity code is transferred between internal processes running on different servers.

14. (**Previously presented**) The method of claim 22 wherein the process comprises a process information vector, and the association of the session identification code to the process comprises adding an identification code of the original session to the process information vector.

15. (**Previously presented**) The method of claim 14 wherein the identification code replaces redundant information in the process information vector.

16. (**Previously presented**) The method of claim 22 wherein the processes are associated to the original session by a unique process identifier.

17. (**Previously presented**) The method of claim 22 wherein the original session properties are sign in parameters.

18. (**Previously presented**) The method of claim 22 wherein the original session properties are initial session type parameters.

19. (**Previously presented**) The method of claim 22 wherein the original session properties are hyperlink session address type parameters.

20. (**Previously presented**) The method of claim 22 wherein the original session is associated with a unique Transmission Control Protocol (TCP) port ID.

21. (**Currently Amended**) A security system comprising:

a server having an operating system, said server communicates with a multiplicity of client users via at least one communication network, wherein the client users initiate original sessions, each of which operates a sequence of processes, said sequence including one or more processes running only the operating system of the server and at least one process of interaction between the a client terminal and the server; and

at least one module operated by said at least one server,

wherein said at least one module associates a session identification code to each original session and to each process in the sequence of processes operated by said original session, wherein said session identification code is related to the manner in which the client user has initiated the original session and is associated with an authorization level,

wherein the server operates the processes in the sequence of processes according to the authorization level associated with the session identification code;

where at least one process in the sequence is an interaction process and at least one succeeding process of said interaction process is operated only at the operating system level of the server, where the module of the server transfers the identification code  between said processes.~~.~~

22. (**Currently Amended**) A computer implemented method for monitoring and controlling communication sessions within a network server environment, wherein each original session operates a sequence of processes,

said method comprising:

- associating each original session with a session identification code;
- associating the identification code of the original session to each process in the sequence operated by the original session ,wherein at least one process is carried out only at the operating system level of a server and at least one process is interaction process between the a client terminal and the server;
- associating an authorization level to the session identification code in accordance with the properties of the original session, wherein the identification code is transferred between at least one interaction process and at least one process operated only at the operating system level which succeeds the  interaction process; and
- operating each process in the process sequence according to the authorization level associated to the session identification code,

wherein said sequence of processes includes operations carried out in the operating system of the server.

23. (**cancelled**)

24. (**Previously presented**) A method of monitoring and/or controlling a communication session within a network server environment,

said method comprising:

- associating the communication session with a session identification code;
- associating an authorization level to the session identification code;
- associating the session identification code of the communication session at least to a child process, said child process been created by a process operated by the communication session; and
- operating the child process according to the authorization level associated with the session identification code.

25. (**Previously presented**) A method according to claim 24, wherein associating the session identification code to the child process comprises

- producing a hierarchical structure of processes at the kernel level; and
- referring each process to the hierarchical tree said each process belongs to.

26. (**Previously presented**) A method according to claim 24, wherein an authorization level is associated to the session identification code in accordance with the properties of the communication session.

27. (**Previously presented**) A security system according to claim 21, wherein one or more of said sequence of processes creates an additional process, and the additional process is associated with the session identification code.

28. (**Previously presented**) A method according to claim 22, wherein one or more of said sequence of processes creates an additional process, and the additional process is associated with the session identification code.